IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of	)
	)
SUZUKI et al.	)
	)
Application Number: To be Assigned	)
	)
Filed: Concurrently Herewith	)
	)
For: NETWORK CONTROL METHOD AND EQUIPMENT	)
	)
ATTORNEY DOCKET NO. HITA.0495	)

Honorable Assistant Commissioner
for Patents
Washington, D.C. 20231

REQUEST FOR PRIORITY
UNDER 35 U.S.C. § 119
AND THE INTERNATIONAL CONVENTION

Sir:

In the matter of the above-captioned application for a United States patent, notice is hereby given that the Applicant claims the priority date of February 10, 2003, the filing date of the corresponding Japanese patent application 2003-031837

A certified copy of Japanese patent application 2003-031837 is being submitted herewith. Acknowledgment of receipt of the certified copy is respectfully requested in due course.

Respectfully submitted,

Stanley P. Fisher
Registration Number 24,344

Juan Carlos A. Marquez
Registration Number 34,072

REED SMITH LLP
3110 Fairview Park Drive
Suite 1400
Falls Church, Virginia 22042
(703) 641-4200
January 16, 2004

310201852 YU

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００３年　２月１０日
出願番号 Application Number:	特願２００３－０３１８３７
[ST. 10/C]:	[ＪＰ２００３－０３１８３７]
出願人 Applicant(s):	株式会社日立製作所

２００３年　９月２６日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３０７９３８８

【書類名】　特許願
【整理番号】　H02018521A
【あて先】　特許庁長官　殿
【国際特許分類】　H04L 12/56
【発明者】
　【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内
　【氏名】　鈴木　伸介
【発明者】
　【住所又は居所】　神奈川県秦野市堀山下１番地　株式会社日立製作所エンタープライズサーバ事業部内
　【氏名】　新　善文
【発明者】
　【住所又は居所】　神奈川県秦野市堀山下１番地　株式会社日立製作所エンタープライズサーバ事業部内
　【氏名】　池田　尚哉
【特許出願人】
　【識別番号】　000005108
　【氏名又は名称】　株式会社　日立製作所
【代理人】
　【識別番号】　100075096
　【弁理士】
　【氏名又は名称】　作田　康夫
　【電話番号】　03-3212-1111
【手数料の表示】
　【予納台帳番号】　013088
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　ネットワーク制御方法及びネットワーク制御装置

【特許請求の範囲】

【請求項１】

ネットワーク内のトラフィックを制御するトラフィック制御装置に接続されるトラフィック制御インタフェースと、

前記トラフィック制御装置でどのようなトラフィック制御が必要かを判断するトラフィック制御要求検出装置に接続されるトラフィック制御要求インタフェースと、

該トラフィック制御要求インタフェースを介して受信されたトラフィック制御に関する情報が格納された第１の記憶手段と、

前記トラフィック制御インタフェース、前記トラフィック制御要求インタフェースおよび前記第１の記憶手段に接続されたトラフィック制御計算部とを有し、

前記トラフィック制御計算部は、第１の記憶手段に格納されたトラフィック制御要求を基にトラフィック制御のアルゴリズムを計算し、前記トラフィック制御インタフェースに送信することを特徴とするトラフィック制御計算装置。

【請求項２】

請求項１に記載のトラフィック制御計算装置において、前記トラフィック制御装置が現在行っているトラフィック制御に関する情報を収集する手段と、

該収集したトラフィック制御に関する情報とトラフィック制御装置のＩＤとが格納された第２の記憶手段とを有することを特徴とするトラフィック制御計算装置。

【請求項３】

請求項１に記載のトラフィック制御計算装置において、前記第１の記憶手段に、前記トラフィック制御要求検出装置のＩＤを格納することを特徴とするトラフィック制御計算装置。

【請求項４】

請求項１に記載のトラフィック制御計算装置において、前記トラフィック制御計算部は、前記トラフィック制御要求インタフェースを介して受信したトラフィ

ック制御要求の要求元を前記第１の記憶手段に記憶されたトラフィック制御情報と照会し、前記受信した要求元が前記第１の記憶手段に格納されていない場合は、前記トラフィック制御要求を棄却することを特徴とするトラフィック制御計算装置。

【請求項５】

請求項４に記載のトラフィック制御計算装置において、更に、ネットワーク管理者との通信窓口となるトラフィック制御計算管理インタフェースを有し、

前記トラフィック制御計算部は、前記受信したトラフィック制御要求と矛盾するトラフィック制御要求が前記第１の記憶手段に含まれていないか判定し、

矛盾したトラフィック制御要求が含まれる場合には、更に該矛盾するトラフィック制御要求の要求元を対比し、

要求元が異なる場合には、前記トラフィック制御計算管理インタフェースへ矛盾を送信することを特徴とするトラフィック制御計算装置。

【請求項６】

請求項５に記載のトラフィック制御計算装置において、前記要求元が同じ場合には、前記トラフィック制御計算部は、前記矛盾した制御要求の削除要求が前記要求元から送信されたと見なすことを特徴とするトラフィック制御計算装置。

【請求項７】

請求項２に記載のトラフィック制御計算装置において、

前記トラフィック制御計算部は、

前記収集する手段による収集が成功した場合には前記トラフィック制御装置が動作していると判断し、

前記格納手段に格納されたトラフィック制御情報を前記新たに収集されたトラフィック制御情報で更新することを特徴とするトラフィック制御計算装置。

【請求項８】

請求項２に記載のトラフィック制御計算装置において、

前記トラフィック制御計算部は、

前記トラフィック制御に関する情報の収集に失敗した場合には前記トラフィック制御装置が動作していないと判断し、

前記格納手段に格納された、前記動作していないと判断されたトラフィック制御装置に対応するトラフィック制御情報を削除することを特徴とするトラフィック制御計算装置。

【請求項９】

ネットワーク内のトラフィックを制御するトラフィック制御装置に接続されるトラフィック制御インタフェースと、

前記トラフィック制御装置でどのようなトラフィック制御が必要かを判断するトラフィック制御要求検出装置に接続されるトラフィック制御要求インタフェースと、

接続されたトラフィック制御要求検出装置のＩＤと装置の持つ検出機能とが格納されたトラフィック制御要求リストと、

該トラフィック制御要求インタフェースを介して受信されたトラフィック制御に関する情報と該情報に対応するトラフィック制御要求検出装置のＩＤとが格納されたトラフィック制御要求リストと、

接続されたトラフィック制御要求検出装置のＩＤと機能とを記載したトラフィック制御要求検出装置リストと、

接続されたトラフィック制御装置のＩＤと機能とが記載されたトラフィック制御装置リストと、

接続されたトラフィック制御装置のＩＤと現時点で実行している制御内容とが記載されたトラフィック制御方法リストと、

前記トラフィック制御要求リストに記載された制御要求に基づき、制御アルゴリズムを計算するトラフィック制御計算部とを有することを特徴とするトラフィック制御計算装置。

【請求項１０】

ネットワーク内のトラフィックを制御するトラフィック制御装置と、ネットワーク内でどのようなトラフィック制御が必要かを検出するトラフィック制御要求検出装置とに接続されたトラフィック制御計算装置の制御方法であって、

トラフィック制御要求を受信し、該受信したトラフィック制御要求と該要求の要求元を示す情報とを記憶手段に格納し、前記受信したトラフィック制御要求が

前記記憶手段に格納された制御要求と矛盾がないかどうか判断し、矛盾が無い場合には、前記制御要求に相当する制御アルゴリズムを計算することを特徴とするトラフィック制御計算装置の制御方法。

【請求項１１】

請求項１０に記載のトラフィック制御計算装置の制御方法において、前記矛盾が存在する場合には、更に、前記受信した要求の要求元と当該矛盾する制御要求の要求元が同じか否かを判断し、

要求元が同じ場合には、前記矛盾する制御要求を前記記憶手段から削除することを特徴とするトラフィック制御計算装置の制御方法。

【請求項１２】

請求項１０に記載のトラフィック制御計算装置の制御方法において、前記矛盾が存在する場合には、更に、前記受信した要求の要求元と当該矛盾する制御要求の要求元が同じか否かを判断し、

要求元が異なる場合には、前記矛盾が存在することをネットワーク管理者へ通知し、当該ネットワーク管理者の判断により矛盾を解決することを特徴とするトラフィック制御計算装置の制御方法。

【請求項１３】

請求項１１に記載のトラフィック制御計算装置の制御方法において、受信したトラフィック制御要求の要求元が予め登録された要求元からの要求であるか否かを判断し、

登録された要求元以外からの制御要求を棄却することを特徴とするトラフィック制御計算装置の制御方法。

【請求項１４】

請求項１３に記載のトラフィック制御計算装置の制御方法において、前記受信したトラフィック制御要求の要求元が予め登録された要求元であった場合には、前記受信したトラフィック制御要求が前記記憶手段に格納された制御要求と矛盾がないかどうかの判断を開始することを特徴とするトラフィック制御計算装置の制御方法。

【請求項１５】

請求項１２に記載のトラフィック制御計算装置の制御方法において、前記ネットワーク管理者が矛盾する制御要求の一部または全てが却下したか否かの情報を受信し、

却下された制御要求の要求元に制御要求が却下された旨を通知することを特徴とするトラフィック制御計算装置の制御方法。

【請求項１６】

請求項１０に記載のトラフィック制御計算装置の制御方法において、該計算装置に接続されたトラフィック制御装置が備える制御アルゴリズムと、前記計算された制御アルゴリズムとを比較し、

前記計算された制御アルゴリズムが前記トラフィック制御装置が備えていない制御アルゴリズムである場合には、該計算された制御アルゴリズムを前記トラフィック制御装置へ送信することを特徴とするトラフィック制御計算装置の制御方法。

【請求項１７】

トラフィック制御要求を受信し、該受信したトラフィック制御要求と該要求の要求元を示す情報とを記憶手段に格納し、前記受信したトラフィック制御要求が前記記憶手段に格納された制御要求と矛盾がないかどうか判断し、矛盾が無い場合には、前記制御要求に相当する制御アルゴリズムを計算し、該計算された制御アルゴリズムに基づいてトラフィック制御を行なうことを特徴とするネットワーク制御方法。

【請求項１８】

ネットワーク内のトラフィックを制御するトラフィック制御装置と、ネットワーク内でどのようなトラフィック制御が必要かを検出するトラフィック制御要求検出装置と、前記検出されたトラフィック制御要求に基づきトラフィック制御要求を処理するトラフィック制御計算装置とを備えたネットワークの制御方法であって、

前記トラフィック制御計算装置を用いて、

前記トラフィックトラフィック制御要求検出装置の識別情報と当該トラフィック制御要求検出装置が備える検出機能を示す情報と当該トラフィック制御要求検

出装置が現在要求しているトラフィック制御要求に関する情報とを受信し（以下、第１の情報とする）、

該収集した第１の情報を記憶手段に格納し、

前記トラフィックトラフィック制御要求検出装置が新たなトラフィック制御を要求した場合に、前記トラフィック制御計算装置は、

新たに受信したトラフィック制御要求が前記第１の記憶手段に格納されたトラフィック制御要求と矛盾しないかどうか判断し、

矛盾がない場合には、受信したトラフィック制御要求に基づき制御アルゴリズムを計算し、

該計算した制御アルゴリズムを前記トラフィック制御装置へ送信することを特徴とするネットワークの制御方法。

【請求項１９】

請求項１８に記載のネットワークの制御方法において、

前記トラフィック制御装置の識別情報と当該トラフィック制御装置が備えているトラフィック制御機能を示す情報とを収集し（以下、第２の情報とする）、

前記収集した第２の情報を記憶手段に格納し、

前記トラフィック制御計算装置が計算した制御アルゴリズムが、前記トラフィック制御装置に既に備えられている場合には、前記送信を行なわないことを特徴とするネットワークの制御方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、インターネットにおける通信制御技術に関し、特にファイアウォール技術に関する。

【０００２】

【従来の技術】

企業ネットワーク等の内部ネットワークにおいてインターネットを利用する際には、一般にファイアウォールが内部ネットワークとインターネットとの境界に導入される。インターネットから内部ネットワークへの不正アクセスを防止する

ためである。

【０００３】

上記ファイアウォールでは、外部からの内部ネットワークへのアクセスは全て不正アクセスであることが前提とされている。しかしながら昨今の常時接続やIPv6によるEnd-to-End通信などの普及に伴い、この前提は内部ネットワークユーザのニーズから外れつつある。例えば出張先から内部ネットワークへアクセスすることや在宅勤務で自宅から内部ネットワークへアクセスすることも不正アクセスとして数えられてしまうためである。

【０００４】

このようなファイアウォールの一例として、米国特許第6233686号には、不正侵入検知システム連動型パケットフィルタ技術が開示されている。当該発明の概要を図６(a)に示す。当該発明では、パケットフィルタに認証サーバが接続されており、認証サーバは、更にパケットフィルタリングの規則が予め登録されたユーザ毎に格納されたデータベースに接続されている。外部からネットワーク内にアクセスしようとする外部端末は、まず認証サーバにログインする。認証サーバは、アクセス要求のあった端末が不正な端末でないと判断すれば、ユーザに対応するパケットフィルタリング規則をデータベースに問い合わせる。問い合せの際には、ログインされたユーザ名を用いる。データベースは、ログインしたユーザに対応するパケットフィルタリング規則を検索し、認証サーバに通知する。認証サーバは、パケットフィルタにデータベースから転送されたフィルタリング規則を転送し、これによって、パケットフィルタは、アクセス要求のあったユーザ毎にパケットフィルタリングの規則を変更することができる。

また、不正アクセスの意志を持ったユーザがログインに成功する場合もある。このような場合、ネットワーク内にパケットモニタリング装置を設けることにより、予め定義された不正アクセスと見なされるパターンを持ったパケットを検出することができる。パケットフィルタは、不正アクセスと見なされるパケットを検出すると、データベースに新たなフィルタリング規則を要求し、フィルタリング規則を変更し、不正パケットを自動的にフィルタリングする。ログインに失敗したユーザからの送信パケットは、パケットフィルタにより廃棄される。

また、学会発表論文 "Distributed Firewalls", ;login:, November 1999, pp. 39-47, Steven Bellovin"および"Controlling High Bandwidth Aggregates in the Network", Computer Communications Review Vol. 32 No.3, pp.62-73, July 2002, Ratul Mahajan, Steve Bellovin, et.al"には、分散ファイアウォール及び集約式輻輳制御に関する技術が開示されている。本文献に開示された技術の概要を図６(b)に示す。これらの文献に記載されたモデルでは、内部ネットワークとインターネットとの境界にパケットフィルタなどの装置は設置しない。そのかわり端末側にパケットフィルタやWebコンテンツフィルタなどのファイアウォール機能(パーソナルファイアウォール)を実装する。パーソナルファイアウォールはポリシーサーバに接続されており、パーソナルファイアウォールの設定条件はポリシーサーバにて一括管理されている。トラフィックの状況は端末側で検出する。端末は、トラフィック異常を検出すると、ポリシーサーバにフィルタリングポリシーを要求する。ポリシーサーバは、予め登録されたフィルタリングポリシーを各端末に配布する。フィルタリングポリシーを受信した端末は、当該ポリシーに基づくフィルタリングの実行をトラフィックの上流側のルータへ通知する。これにより、異常トラフィックの発生時に、ネットワーク全体でファイアウォール機能が実現できる。

【０００５】

【発明が解決しようとする課題】

特に常時接続やIPv6によるEnd-to-End通信の普及によりインターネットには質的な変化が訪れようとしている。具体的には、Instant Messageに代表されるPeer to Peerアプリケーションの普及、公衆無線LANサービスの普及によるユーザとIPアドレスとの対応付けの困難化、マルチキャストやVoice over IPに代表されるリアルタイム性を要求するトラフィックの増加、DoS(Denial of Service)攻撃の深刻化、IPsecの普及による暗号化通信、IP接続された端末の増加に伴うフィルタリング対象トラフィック数の増大といったものである。

【０００６】

従来のファイアウォール技術ではこうした質的な変化に追従することができない。例えば、米国特許6233686号に開示された技術では、暗号化通信のフィルタ

リングが出来ない。暗号化されたパケットは中身をみることができないため、認証サーバがフィルタリング規則をデータベースへ問い合わせることができないためである。また、DoS攻撃に対する耐性もない。トラフィック制御の方法が認証しかないため、一旦認証されれば、不正なパケットでもネットワーク内部にアクセス可能となるためである。

【０００７】

また、米国特許6233686号の発明に不正侵入検知システムを組み合わせても、暗号化通信のフィルタリングやアプリケーションの多様化への対応は事実上不可能である。内部ネットワークへのアクセスが認められたパケットが不正なパケットと判明した場合、不正アクセス検出装置は、トラフィック制御装置（例えばルータ）に対して、不正パケットのアクセスを禁止するフィルタリングルールを追加しようとする。しかし、通常、ルータ等のトラフィック制御装置では、先に入力されたパケットのアクセスを認める設定が有効になるため、一旦認証されたパケットの、事後によるアクセス制限は困難である。したがって、米国特許6233686号に記載の発明と不正侵入検知システムを組み合わせたネットワークシステムでも、暗号化通信のフィルタリングやアプリケーションの多様化への対応は不可能である。

【０００８】

次に、前記の学会発表論文に記載された分散ファイアウォールアーキテクチャでは、企業ネットワークのみならず外部にある全ての端末にパーソナルファイアウォールを実装する必要がある。したがって、ネットワークの規模が大きくなり、フィルタリング対象トラフィック数が増大すると、システム構築のコストが増大する。また、ポリシーサーバは、予め定められたフィルタリングポリシーを全ての端末に一方的に配信する装置である。したがって、複数のファイアウォール技術が互いに矛盾した制御を行う場合や、個々のパケットフィルタ技術が互いに相容れないものである場合には、ポリシーサーバによっては、ネットワークの整合を勘案したトラフィック制御を行うことが出来ない。

【０００９】

更にまた、いずれの技術も、フィルタリング対象トラフィック数の増大による

フィルタリングルール数の増大のために制御装置の負荷が大きくなるという問題を含んでいる。

【００１０】

以上、インターネットに発生する問題群を同時に解決するファイアウォール技術は存在しない。しかも従来のファイアウォール技術を単純に複数組み合わせてはこれらの問題群を同時解決することはできない。複数のファイアウォール技術が互いに矛盾した制御を行う場合や、そもそも個々のパケットフィルタ技術が互いに相容れないものである場合には対応できないからである。

【００１１】

上述の課題を一般化して説明すると、複数のトラフィック制御要求装置によりトラフィック制御を行う場合には、トラフィック制御要求装置は自らのトラフィック制御要求をトラフィック制御装置に伝えるのみならず、同じトラフィック制御装置への他の制御要求装置からの制御要求を抑止しなければならないということである。

【００１２】

本発明の目的は、複数のファイアウォール技術の連係を一箇所に集約して自動化することにより、この問題を解決する枠組みを提供することである。

【００１３】

【課題を解決するための手段】

本発明のネットワーク制御装置の構成は、ネットワーク内においていずれのトラフィックを通したり弾いたりするかの判断材料を提供するトラフィック制御要求検出装置と、ネットワークのトラフィックを実際に制御するトラフィック制御装置と、トラフィック制御装置からの制御要求を処理するトラフィック制御計算装置とを含んでいる。

【００１４】

トラフィック制御要求計算装置は、トラフィック制御要求検出装置からトラフィック制御要求を受信すると、受信したトラフィック制御要求を記憶手段に格納する。次に、トラフィック制御要求計算装置は、格納された制御情報を基に、接続されたトラフィック制御装置で、トラフィック制御をどのように実現すべきか

を、トラフィック制御装置群の機能や現在行っている制御設定などを基に算出する。

【００１５】

一方、トラフィック制御要求計算装置は、管理対象であるトラフィック制御装置群からトラフィック制御に関するトラフィック制御情報も収集する。収集されたトラフィック制御情報は格納手段に格納される。装置の初動時の際には、トラフィック制御計算装置は、トラフィック制御装置に設定された初期設定を収集・学習することになる。

【００１６】

ネットワーク内にトラフィック制御装置が複数配置されている場合には、各トラフィック制御装置からの制御要求が矛盾する場合がありうる。このような場合、トラフィック制御計算装置は、各ネットワーク制御装置から要求された制御要求を調整し、ネットワーク制御装置全体の動作に支障が無いようにする。また、本発明のトラフィック制御計算装置は、複数のトラフィック制御要求装置からのトラフィック制御要求を一括して処理することにより、この課題を克服する。これにより他のトラフィック制御技術との親和性が確保される。

【００１７】

【発明の実施の形態】

（実施例１）

以下本発明の実施形態を具体的に説明する。

【００１８】

なお、本実施例におけるトラフィック制御要求検出装置の具体例としては、例えば、異常トラフィックを検知する不正侵入検知システム、ユーザ認証型ファイアウォールにおけるユーザ認証サーバ、分散ファイアウォールにおけるポリシーサーバ等が該当する。また、トラフィック制御装置の具体例としては、例えば、パケットフィルタ、トラフィックシェーパ、アプリケーションゲートウェイ、パーソナルファイアウォール等が該当する。トラフィック制御要求検出装置とトラフィック制御要求計算装置、およびトラフィック制御装置とトラフィック制御要求計算装置間は、管理用ネットワークや暗号化通信などを用いて安全に通信でき

る状態にあることが好ましい。

【００１９】

図１には、一般的なパケットフィルタ装置の動作を示す。パケットフィルタ100は回線110からパケットの入力を受けると、まず入力パケットフィルタ120にて入力パケットと入力パケットフィルタリングルールとのマッチングをとることにより、そのパケットを通すか否かを決定する。具体的にはパケットの中のIPアドレスやポート番号やプロトコル種別などを、それぞれパケットフィルタリングルールの各ルールと照らし合わせ、合致したルールに従ってパケットを通過させるか否かを決定する。パケットを通過させないと判定されたときには入力パケットフィルタ120にて入力されたパケットは棄却され、通過させると判定されたときには入力されたパケットはパケット中継処理部130の処理に従ってしかるべき出力インタフェース150へ出力される。出力インタフェース150へパケットが出力される前に、パケットは出力パケットフィルタ140によって出力されるか否かが決定される。その判定基準は入力パケットの場合と同様である。そして出力すると判定された場合にパケットは出力インタフェース150へ出力される。すなわち入力パケットフィルタリングルールと出力フィルタリングルールとを適切に指定することによって、パケットフィルタ100は適正なパケットのみをインターネットから企業ネットワークへ中継することができるのである。しかしながらそのフィルタリングルールをインターネットからの接続要求や異常アクセスの動向に応じて適切に設定することは従来技術では困難である。また送信者と受信者以外がパケットの中身を見ることができない暗号化通信に対しては、この装置を適用することは難しい。

【００２０】

図2には、本実施例のトラフィック制御システムの全体図を示す。まず、トラフィック制御計算装置230がネットワーク上に配置されている。トラフィック制御計算装置230は、トラフィック制御要求インタフェース240およびネットワーク回線（引出番号は記されていない）を介してトラフィック制御要求検出装置210ならびに215と接続されている。この際、トラフィック制御計算装置230とトラフィック制御要求検出装置210ならびに215との間には通信上のセキュリティが確保

されていることが望ましく、210、215、230間の通信は、管理用ネットワークや暗号化通信などを用いることが特に好ましい。トラフィック制御計算装置230と接続されているトラフィック制御要求検出装置は全てトラフィック制御要求検出装置リスト260に記載されている。

【００２１】

同様に、トラフィック制御計算装置230は、トラフィック制御装置220ならびに225と接続されている。トラフィック制御インタフェース245およびネットワーク回線を介して接続されている。トラフィック制御計算装置230と接続されているトラフィック制御装置は、全てトラフィック制御装置リスト265に記載されている。トラフィック制御計算装置230内には、トラフィック制御要求検出装置210、215からのトラフィック制御要求が格納されるトラフィック制御要求リスト250、トラフィック制御要求リスト250の内容を基に算出されたトラフィック制御方法リスト255、そして全体を統括するトラフィック制御計算部270が設けられている。これらのリストは、トラフィック制御計算装置230内に設けられた記憶手段、例えば、半導体メモリ、レジスタ、あるいはハードディスクなどの外部記憶装置に格納される。リストを格納する際には、一つの記憶手段に全てのリストを格納しても良いし、リスト毎に記憶手段を設けても構わない。トラフィック制御計算部は、トラフィック制御計算装置230の筐体内に設けられたプロセッサ、マイコンないしこれらの計算器が実装された基板等により実現される。トラフィック制御計算部270にはネットワーク管理者がトラフィック制御計算に介入するためのトラフィック制御計算管理インタフェース280が付随している。ここで、トラフィック制御要求検出装置リスト260およびトラフィック制御装置リスト265は、実際にその装置でどのような処理が実行できるかを示すリストであり、一方、トラフィック制御要求リスト250は当該装置で現在どのような処理が要求されているか、およびトラフィック制御方法リスト255は当該装置で現在どのような処理が実行されているかを示すリストである。トラフィック制御要求検出装置リスト260およびトラフィック制御装置リスト265は不正入力を防ぐために必要な情報であり、トラフィック制御要求リスト250およびトラフィック制御方法リスト255は、状態管理のために必要な情報である。

【００２２】

以下には、図２に記載した装置およびネットワークシステムの動作について説明する。トラフィック制御要求検出装置210、215は、当該装置に接続された回線の状態を監視し、どのようなトラフィック制御が必要かを判断する。必要なトラフィック制御を判断した後、トラフィック制御要求検出装置210、215は、トラフィック制御計算装置230へ必要な制御を通知する。

【００２３】

トラフィック制御計算装置230は、トラフィック制御要求を受け取ると、トラフィック制御要求リスト250を更新する。トラフィック制御計算装置230に接続された各トラフィック制御要求検出装置にはＩＤが附されており、リスト250を更新する際には、検出装置のＩＤと実際に要求されている制御が格納される。また、当該トラフィック制御が必要な理由も、リスト250に書き込まれる。

【００２４】

リスト250を更新する際には、トラフィック制御要求検出装置リスト260が参照される。トラフィック制御計算部270は、リスト250を更新する際に、リスト260を参照し、通知されたトラフィック制御要求の要求元のＩＤがリスト260に記載されていない場合、当該制御要求は不正な要求と判断し、要求を棄却する。

【００２５】

次に、トラフィック制御要求計算部270は、リスト250に格納されたトラフィック制御要求を基に、接続されたトラフィック制御装置220や225で必要となるトラフィック制御のアルゴリズムを計算する。あるいは、接続されたトラフィック制御装置の数に応じて複数の制御アルゴリズムを用意しておき、トラフィック制御要求検出装置210、215から要求されたトラフィック制御に応じて、適切なアルゴリズムを選択するようにしても良い。

【００２６】

計算ないし選択された制御アルゴリズムは、トラフィック制御インタフェースを介してトラフィック制御装置220、225に送信される。

【００２７】

トラフィック制御装置220、225は、送信された制御アルゴリズムに応じて、ト

ラフィック制御を行う。

【００２８】

図3のフローチャートには、トラフィック制御計算装置230がトラフィック制御装置から情報収集する方法を示した。トラフィック制御計算装置230は、トラフィック制御装置リスト265に記載されている全てのトラフィック制御装置について、現時点で実行しているトラフィック制御内容を取得する。具体的にはトラフィック制御装置の構成定義をトラフィック制御インタフェース245を介して取得することにより実現される(ステップ300)。制御内容が取得できた場合には、該当トラフィック制御装置の制御内容をトラフィック制御方法リスト255に保管する(ステップ320)と同時に、トラフィック制御装置リスト265内の該当トラフィック制御装置エントリの稼働中フラグ268をONにする(ステップ325)。逆に制御内容が取得できなかった場合には、トラフィック制御方法リスト255から該当トラフィック制御装置のトラフィック制御方法エントリを削除する(ステップ330)と共に、トラフィック制御装置リスト265内の該当トラフィック制御装置エントリの稼働中フラグ268をOFFにする(ステップ335)。

【００２９】

図4のフローチャートには、トラフィック制御計算装置230がトラフィック制御要求検出装置リストに記載された要求（IDは210ならびに215）からの要求を処理する方法を示した。トラフィック制御要求インタフェース240がトラフィック制御要求を受信すると、その要求を出したトラフィック制御要求検出装置がトラフィック制御要求検出装置リスト260に含まれているかをチェックする(ステップ410)。もし含まれていなければ、そのトラフィック制御要求は不正なものと判断して、却下される(ステップ415)。含まれている場合には正当なトラフィック制御要求であると判断する。そして過去にそのトラフィック制御要求検出装置から発生した制御要求の中に、新たに入力された制御要求と反対の内容のエントリがあるか否かを確認する(ステップ420)。それが存在する場合には、そのエントリが同じトラフィック制御要求検出装置から発生しているか否かを判定する(ステップ425)。

【００３０】

同じトラフィック制御要求検出装置から発生しているならば、そのエントリを新しいトラフィック制御要求により上書きし(ステップ430)、違っている場合にはその旨を管理インタフェースを通じてより高次な判断をできるネットワーク管理者(例えば人間や人工知能システム)へ通知する(ステップ432)。その通知を受けたネットワーク管理者はどちらのトラフィック制御要求部を棄却するかを決定し、トラフィック制御計算管理インタフェース280を経由して指示する(ステップ435)。その結果(ステップ440)、新しいトラフィック制御要求が棄却された場合には、トラフィック制御計算装置230はその制御要求を出したトラフィック制御要求検出装置に対してその要求を棄却したことをトラフィック制御要求インタフェース240を通じて通知する(ステップ445)。トラフィック制御要求検出装置はその棄却通知を無視しても、制御要求の基になったユーザ認証などのイベントを取り消すのに使用してもよい。

【００３１】

ステップ440にて、過去のトラフィック制御要求が棄却された場合には、トラフィック制御計算装置230はその棄却要求が直接トラフィック制御要求検出装置から入力されたように動作する(ステップ430)。ステップ420にて制御要求と反対の内容のエントリが存在しない場合には特に何もしない。以上のステップ420の処理が終った後新しい制御要求が棄却されていなければ、新しいトラフィック制御要求をトラフィック制御要求リスト250へ追加する(ステップ450)。

【００３２】

ステップ450にて新たなトラフィック制御要求リストが生成された後、トラフィック制御計算部270は、そのトラフィック制御要求群をトラフィック制御装置リスト265に含まれている稼働中フラグ268がONなトラフィック制御装置群を用いてどのようにして実現するかを計算する(ステップ460)。

【００３３】

計算に際しては、トラフィック制御装置リスト265に記載されているトラフィック制御装置機能267やトラフィック制御方法リスト255に記載されている現時点でのトラフィック制御方法も考慮して、ネットワーク中継性能を最大にするようにトラフィック制御方法を最適化する。最適化方法には、トラフィック制御装置

群間での負荷分散、トラフィック制御装置間での機能分化、トラフィック制御ルール数の最小化などやこれらの複合案がありえる。例えばトラフィック制御装置群間での負荷分散を行うには、トラフィック制御方法リスト255におけるトラフィック制御装置単位のトラフィック制御情報258の数が均等になるようにトラフィック制御情報を実現するトラフィック制御装置を振り分ければよい。またトラフィック制御装置間の機能分化を行うには、例えばTCP/UDP情報でのフィルタリングはトラフィック制御装置220で行わせ、URLでのフィルタリングはトラフィック制御装置225で行わせるという具合に、トラフィック制御情報に記述されたトラフィックの種類によりそれを実行するトラフィック制御装置を振り分ければよい。どのような最適化方法をとるかはネットワーク管理者の判断するところであり、事前にトラフィック制御計算管理インタフェース280を通じてトラフィック制御計算部270へ定義されているものとする。

【００３４】

ステップ460にてトラフィック制御の実現方法を計算し終った後、トラフィック制御計算装置230はトラフィック制御方法リストと過去のトラフィック制御方法リスト255とを比較し、差分を抽出する(ステップ470)。そしてその差分リストの内容の実行をそれぞれ該当するトラフィック制御装置へトラフィック制御インタフェース245を経由して要求する(ステップ480)。最後に、実行要求完了後トラフィック制御方法リスト255を新たなトラフィック制御方法リストで上書きする(ステップ490)。トラフィック制御装置は、以前に送られた制御アルゴリズムは記憶しているため、新たに送信する制御アルゴリズムは、差分データのみで構わない。

（実施例２）

図5に、本発明を用いたネットワーク構築事例を示す。企業ネットワーク500の中には、対外接続ルータ510、トラフィック制御ルータ520、認証サーバ530、不正侵入検知システム540、分散ファイアウォールポリシーサーバ550、分散ファイアウォール入り端末560が含まれている。そしてトラフィック制御計算装置230が、トラフィック制御要求インタフェース240を介して認証サーバ530や不正侵入検知システム540や分散ファイアウォール入り端末560と、トラフィック制御インタ

フェース245を介して対外接続ルータ510やトラフィック制御ルータ520や分散ファイアウォールポリシーサーバ550と接続されている。

【００３５】

企業ネットワーク外にある端末570から企業ネットワーク内の端末560へアクセスするときには、まず認証サーバ530へログインする。ログインが承認されると、ユーザに応じた通信権が認証サーバにより与えられ、その通信を許可する要求がトラフィック制御要求インタフェース240を介してトラフィック制御計算装置230へ通知される。トラフィック制御計算装置230は図4のフローチャートに従いその制御要求を処理し、トラフィック制御ルータ520にて端末560と端末570との間の通信を許可すると同時に分散ファイアウォールポリシーサーバ550へ、端末560に端末570との通信を許可するよう指示する。

【００３６】

以下には、ネットワークシステム550が端末570を用いたDoSアタックを受けた場合のトラフィック制御計算装置の具体的な動作について説明する。端末570によるDoSアタックを不正侵入検知システム540が検知すると、不正侵入検知システム540からトラフィック制御要求インタフェース240を介してその通信を停止する要求がトラフィック制御計算装置230へ通知される。トラフィック制御計算装置230は図4のフローチャートに従い制御要求を処理した結果、認証サーバ530からの要求と不正侵入検知システム540からの要求との矛盾を検出する。この場合トラフィック制御計算装置230はネットワーク管理者にトラフィック制御計算管理インタフェース280を通じてメールなどの手段により警告を促す。ネットワーク管理者はこの警告に対してどのような処理を行うべきか判断して、トラフィック制御計算装置230にトラフィック制御計算管理インタフェース280を介して指示する。

【００３７】

例えば、仮に管理者がトラフィック制御ルータ520にて当該トラフィックの帯域を絞ることにより対応すると決定した場合には、その旨をトラフィック制御計算管理インタフェース280を介して入力することによりトラフィック制御ルータ520が所望の動作をするようになる。また、端末570が端末560のシステム破壊を試

みていることが端末560のパーソナルファイアウォールにより検知されたときには、パーソナルファイアウォールからその旨がトラフィック制御計算装置230へ通知される。通常、この場合にはトラフィック制御計算装置230は特に新たなトラフィック制御をかける必要はないが、トラフィック制御要求リスト250に余りに大量に同じ要求が含まれている場合その通信は遮断されることが望ましい。その場合トラフィック制御計算装置230は図4のフローチャートに従い、その通知を基にその通信を遮断するような制御方法を計算する。その結果認証サーバ530に対してログイン要求を却下する旨を通知すると同時に、トラフィック制御ルータ520にてその通信を通過させるパケットフィルタを削除し不要になった帯域制御も中止させる。

【００３８】

【発明の効果】

本発明のトラフィック制御計算装置を導入することにより、不正アクセスや正当なアクセス要求に応じた適切なトラフィック制御を既存トラフィック制御装置を組み合わせて柔軟に実現することができるようになる。これにより企業ネットワークを外部から使用するときの利便性を安全に向上させることができるようになり、企業ネットワークユーザは、在宅勤務の促進やバーチャルオフィス化の推進などといった、常時接続やIPv6の普及に伴う恩恵を受けることができるようになる。

【図面の簡単な説明】

【図１】

一般的なパケットフィルタの構造を示す。

【図２】

本発明のシステム全体図を示す。

【図３】

本発明において、トラフィック制御計算装置230がトラフィック制御装置から制御情報を収集する方法を示す。

【図４】

本発明により、トラフィック制御計算装置230がトラフィック制御要求検出装

置からの制御要求を基に、トラフィック制御装置を制御する方法を示す。

【図５】

本発明を用いたネットワーク構築事例を示す。

【図６】

従来技術の説明図である。

【符号の説明】

210 トラフィック制御要求検出装置

215 トラフィック制御要求検出装置

220 トラフィック制御装置

225 トラフィック制御装置

230 トラフィック制御計算装置

240 トラフィック制御要求インタフェース

245 トラフィック制御装置インタフェース

250 トラフィック制御要求リスト

255 トラフィック制御方法リスト

260 トラフィック制御要求検出装置リスト

265 トラフィック制御装置リスト

270 トラフィック制御計算部

280 トラフィック制御計算管理インタフェース

510 対外ルータ

520 トラフィック制御ルータ

530 認証サーバ

540 不正侵入検出システム

550 分散ファイアウォールポリシーサーバ

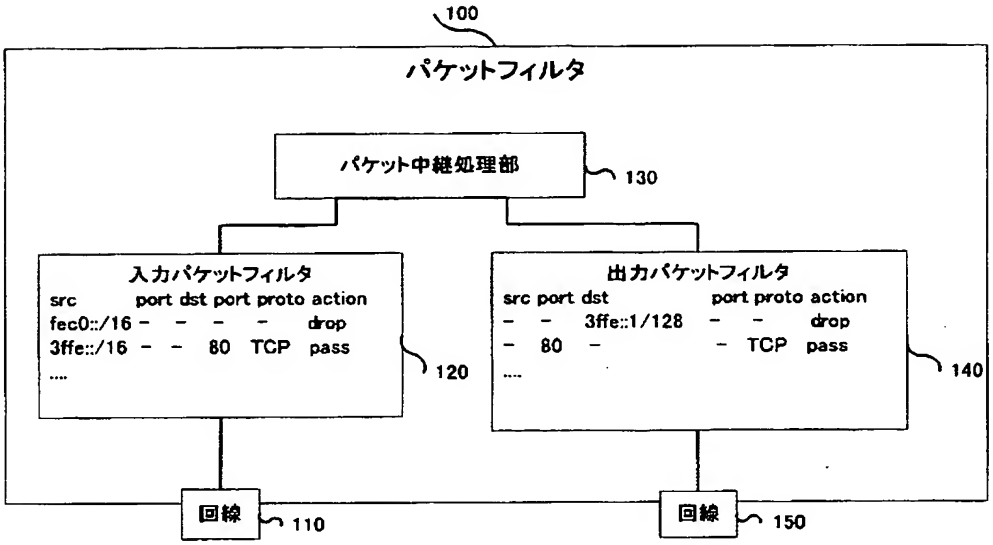
560 端末

570 端末。

【書類名】　図面

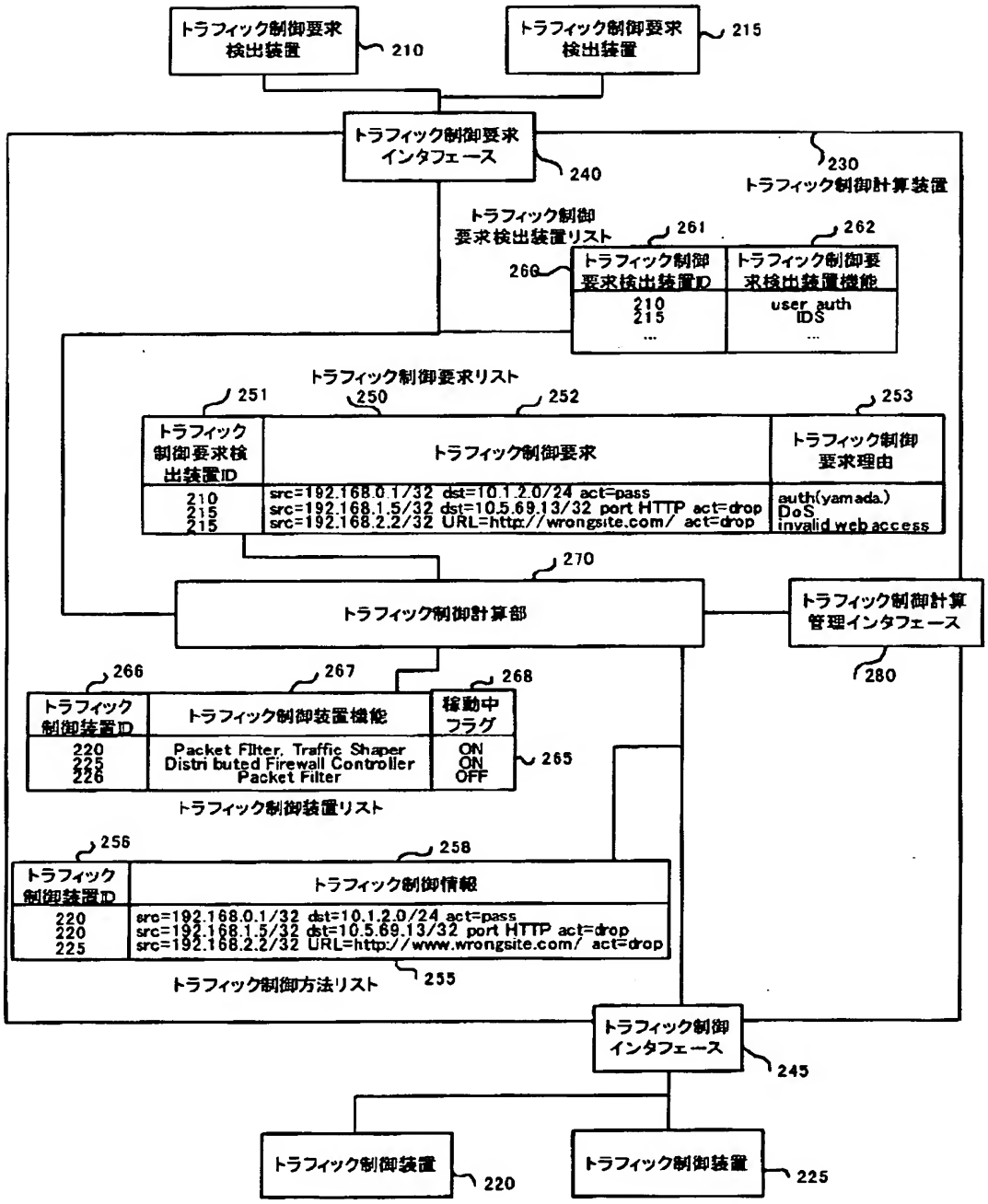
【図１】

図１


100
パケットフィルタ
パケット中継処理部
130
入力パケットフィルタ
src port dst port proto action
fec0::/16 - - - - drop
3ffe::/16 - - 80 TCP pass
....
120
出力パケットフィルタ
src port dst port proto action
- - 3ffe::1/128 - - drop
- 80 - - TCP pass
....
140
回線
110
回線
150

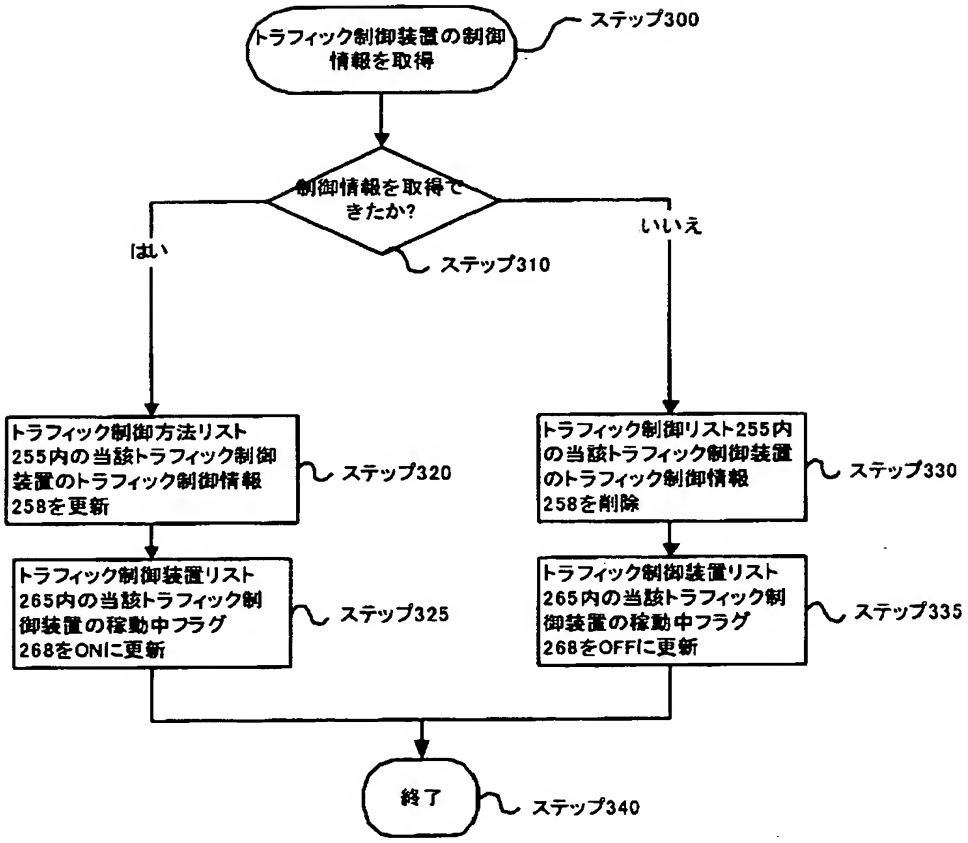
【図２】

図２


トラフィック制御要求検出装置
210
トラフィック制御要求検出装置
215
トラフィック制御要求インタフェース
240
230
トラフィック制御計算装置
トラフィック制御要求検出装置リスト
261
262
260
トラフィック制御要求検出装置ID
トラフィック制御要求検出装置機能
210
215
...
user_auth
IDS
...
トラフィック制御要求リスト
251
250
252
253
トラフィック制御要求検出装置ID
トラフィック制御要求
トラフィック制御要求理由
210
215
215
src=192.168.0.1/32 dst=10.1.2.0/24 act=pass
src=192.168.1.5/32 dst=10.5.69.13/32 port HTTP act=drop
src=192.168.2.2/32 URL=http://wrongsite.com/ act=drop
auth(yamada.)
DoS
invalid web access
270
トラフィック制御計算部
トラフィック制御計算管理インタフェース
280
266
267
268
トラフィック制御装置ID
トラフィック制御装置機能
稼動中フラグ
220
225
226
Packet Filter, Traffic Shaper
Distributed Firewall Controller
Packet Filter
ON
ON
OFF
265
トラフィック制御装置リスト
256
258
トラフィック制御装置ID
トラフィック制御情報
220
220
225
src=192.168.0.1/32 dst=10.1.2.0/24 act=pass
src=192.168.1.5/32 dst=10.5.69.13/32 port HTTP act=drop
src=192.168.2.2/32 URL=http://www.wrongsite.com/ act=drop
トラフィック制御方法リスト
255
トラフィック制御インタフェース
245
トラフィック制御装置
220
トラフィック制御装置
225

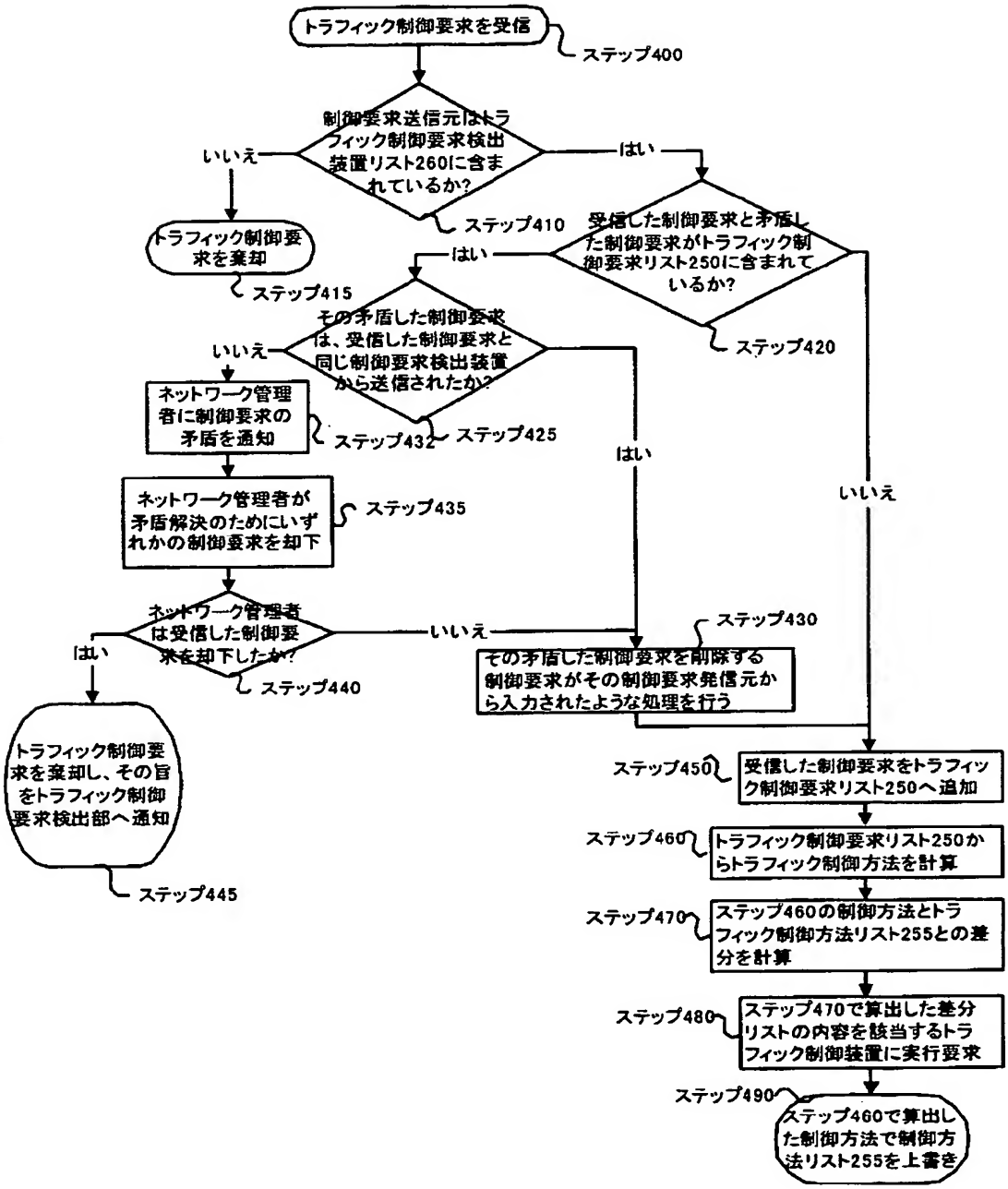
【図３】

図３


トラフィック制御装置の制御情報を取得
ステップ300
制御情報を取得できたか?
ステップ310
はい
いいえ
トラフィック制御方法リスト255内の当該トラフィック制御装置のトラフィック制御情報258を更新
ステップ320
トラフィック制御装置リスト265内の当該トラフィック制御装置の稼動中フラグ268をONに更新
ステップ325
トラフィック制御リスト255内の当該トラフィック制御装置のトラフィック制御情報258を削除
ステップ330
トラフィック制御装置リスト265内の当該トラフィック制御装置の稼動中フラグ268をOFFに更新
ステップ335
終了
ステップ340

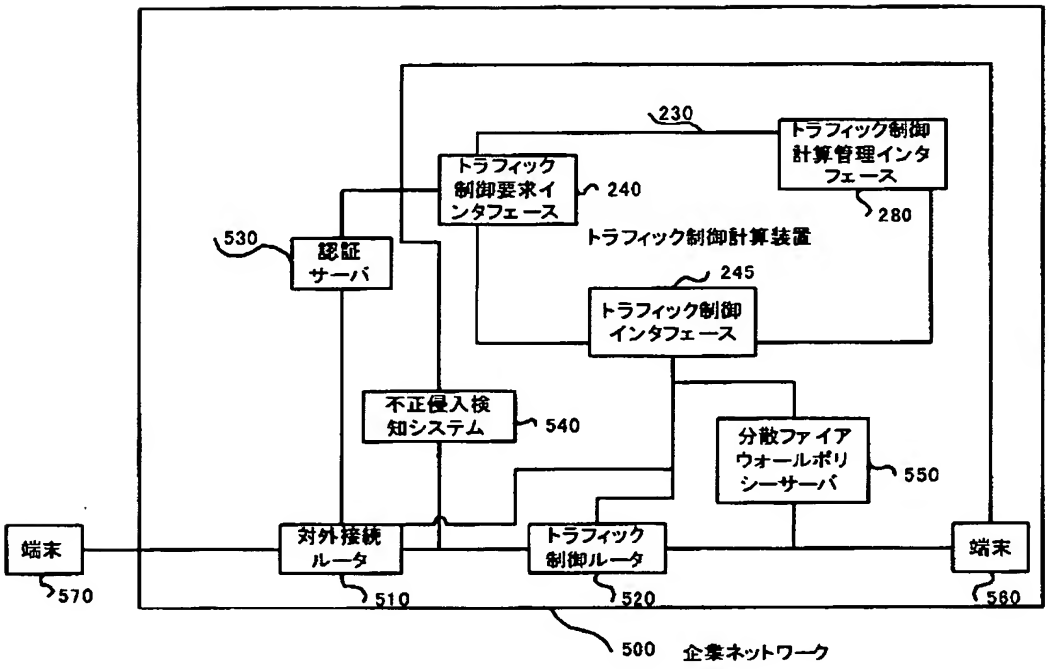
【図４】

図４


トラフィック制御要求を受信
ステップ400
制御要求送信元はトラフィック制御要求検出装置リスト260に含まれているか?
いいえ
はい
ステップ410
トラフィック制御要求を棄却
ステップ415
受信した制御要求と矛盾した制御要求がトラフィック制御要求リスト250に含まれているか?
はい
ステップ420
その矛盾した制御要求は、受信した制御要求と同じ制御要求検出装置から送信されたか?
いいえ
はい
ステップ425
ネットワーク管理者に制御要求の矛盾を通知
ステップ432
ネットワーク管理者が矛盾解決のためにいずれかの制御要求を却下
ステップ435
ネットワーク管理者は受信した制御要求を却下したか?
はい
いいえ
ステップ440
トラフィック制御要求を棄却し、その旨をトラフィック制御要求検出部へ通知
ステップ445
その矛盾した制御要求を削除する制御要求がその制御要求発信元から入力されたような処理を行う
ステップ430
いいえ
ステップ450
受信した制御要求をトラフィック制御要求リスト250へ追加
ステップ460
トラフィック制御要求リスト250からトラフィック制御方法を計算
ステップ470
ステップ460の制御方法とトラフィック制御方法リスト255との差分を計算
ステップ480
ステップ470で算出した差分リストの内容を該当するトラフィック制御装置に実行要求
ステップ490
ステップ460で算出した制御方法で制御方法リスト255を上書き

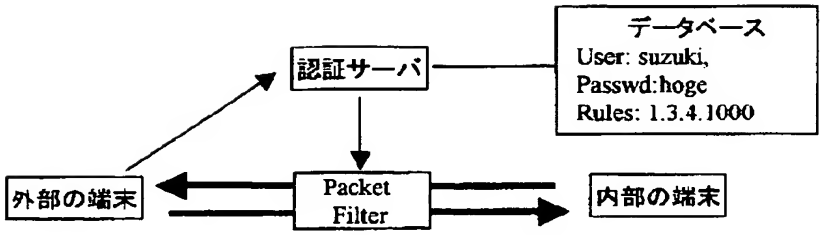
【図５】

図５

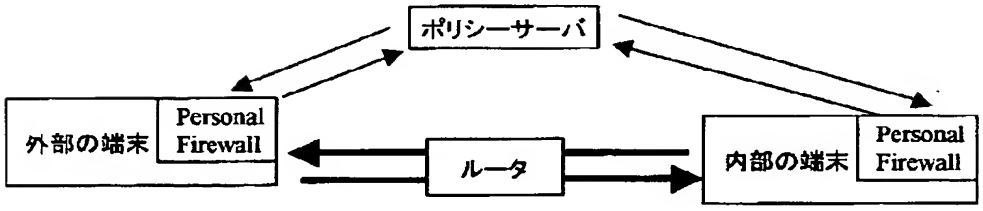

230
トラフィック制御計算管理インタフェース
280
トラフィック制御要求インタフェース
240
トラフィック制御計算装置
530
認証サーバ
245
トラフィック制御インタフェース
不正侵入検知システム
540
分散ファイアウォールポリシーサーバ
550
端末
570
対外接続ルータ
510
トラフィック制御ルータ
520
端末
560
500
企業ネットワーク

【図６】

図６


データベース
User: suzuki,
Passwd:hoge
Rules: 1.3.4.1000
認証サーバ
外部の端末
Packet
Filter
内部の端末

(a)


ポリシーサーバ
外部の端末
Personal
Firewall
ルータ
内部の端末
Personal
Firewall

(b)

【書類名】　　要約書

【要約】

【課題】　複数のファイアウォール技術を組み合わせて、適切に連携させることにより、常時接続やIPv6によるEnd-to-End通信の普及に伴って発生する問題を解決する。これにより企業ネットワークユーザに、在宅勤務、バーチャルオフィス化の推進などといった、常時接続やIPv6の普及に伴う恩恵を与えることにある。

【解決手段】　ネットワーク内にトラフィック制御装置からの制御要求を処理するトラフィック制御計算装置を設けて、個々のトラフィック制御装置の制御動作を適切に連携させる。

【選択図】　図２

認定・付加情報

特許出願の番号	特願２００３－０３１８３７
受付番号	５０３００２０５５２２
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１５年　２月１２日

＜認定情報・付加情報＞

【提出日】　平成15年 2月10日

次頁無

特願２００３－０３１８３７

出　願　人　履　歴　情　報

識別番号　　［０００００５１０８］

１．変更年月日　　１９９０年　８月３１日
［変更理由］　　新規登録
住　所　　東京都千代田区神田駿河台４丁目６番地
氏　名　　株式会社日立製作所